

GetFileNameFromBrowse

Return buffer length should be MAX_PATH length

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-03-23

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4523 bytes

Attack Category	<ul style="list-style-type: none">Malicious Input								
Vulnerability Category	<ul style="list-style-type: none">Buffer OverflowInput source (not really attack)Unconditional								
Software Context	<ul style="list-style-type: none">Shell Functions								
Location	<ul style="list-style-type: none">shlobj.h								
Description	<p>The destination string buffer for GetFileNameFromBrowse() must be long enough to hold the return file path and the returned file path must be validated before use.</p> <p>The GetFileNameFromBrowse() function creates an Open dialog box that lets the user specify the drive, directory, and name of a file to open. The destination string buffer must be long enough to hold the return file path and the returned file path must be validated before use.</p> <p>There is no way to predict the size of the returned filename, so the buffer should be at least MAX_PATH length.</p>								
APIs	<table border="1"><thead><tr><th>Function Name</th><th>Comments</th></tr></thead><tbody><tr><td>GetFileNameFromBrowse</td><td></td></tr><tr><td>GetFileNameFromBrowseA</td><td></td></tr><tr><td>GetFileNameFromBrowseW</td><td></td></tr></tbody></table>	Function Name	Comments	GetFileNameFromBrowse		GetFileNameFromBrowseA		GetFileNameFromBrowseW	
Function Name	Comments								
GetFileNameFromBrowse									
GetFileNameFromBrowseA									
GetFileNameFromBrowseW									
Method of Attack	Buffer Overflow								
Exception Criteria									
Solutions	<table border="1"><thead><tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr></thead><tbody><tr><td>Whenever GetFileNameFromBrowse() is called.</td><td>The second parameter, pszFilePath, must be at least MAX_PATH</td><td>Believed effective, given proper validation of result.</td></tr></tbody></table>	Solution Applicability	Solution Description	Solution Efficacy	Whenever GetFileNameFromBrowse() is called.	The second parameter, pszFilePath, must be at least MAX_PATH	Believed effective, given proper validation of result.		
Solution Applicability	Solution Description	Solution Efficacy							
Whenever GetFileNameFromBrowse() is called.	The second parameter, pszFilePath, must be at least MAX_PATH	Believed effective, given proper validation of result.							

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

	<p>characters in length to ensure that it is large enough to hold the returned string. Otherwise, a buffer overflow can occur. Actually, the documentation does not specify the maximum size for pszFilePath, but we assume MAX_PATH as it is the maximum length of a file path in Windows.</p> <p>Also, the value of pszFilePath returned by this function is the file name specified by the user in the Open dialog, so the value of this file path must be validated before use.</p>
<p>Signature Details</p>	<pre>(HWND hwnd, LPWSTR pszFilePath, UINT cchFilePath, LPCWSTR pszWorkingDir, LPCWSTR pszDefExt, LPCWSTR pszFilters, LPCWSTR szTitle);</pre>
<p>Examples of Incorrect Code</p>	<pre>TCHAR pszFilePath[15]; // Buffer too small [...] // Define and populate other parameters BOOL result = GetFileNameFromBrowse(hwnd, pszFilePath,</pre>

	<pre>cchFilePath, pszWorkingDir, pszDefExt, pszFilters, szTitle);</pre>				
Examples of Corrected Code	<pre>TCHAR pszFilePath[MAX_PATH]; // Buffer correctly sized [...] // Define and populate other parameters BOOL result = GetFileNameFromBrowse(hwnd, pszFilePath, cchFilePath, pszWorkingDir, pszDefExt, pszFilters, szTitle);</pre>				
Source Reference	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/getfilenamefrombrowse.asp ²				
Recommended Resource	MSDN reference for GetFileNameFromBrowse ³				
Discriminant Set	<table border="1"> <tr> <td>Operating System</td> <td> <ul style="list-style-type: none"> Windows </td> </tr> <tr> <td>Languages</td> <td> <ul style="list-style-type: none"> C C++ </td> </tr> </table>	Operating System	<ul style="list-style-type: none"> Windows 	Languages	<ul style="list-style-type: none"> C C++
Operating System	<ul style="list-style-type: none"> Windows 				
Languages	<ul style="list-style-type: none"> C C++ 				

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>